(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 899 733 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
21.03.2001 Bulletin 2001/12

(51) Int Cl.[7]: **G11B 20/00**, G06F 1/00

(21) Application number: **97114927.3**

(22) Date of filing: **28.08.1997**

(54) **Optical disc copy management system**

System zur Kopierverwaltung einer optischen Platte

Système d'administration du copiage de disque optique

(84) Designated Contracting States:
AT DE ES FR GB IE IT NL

(43) Date of publication of application:
03.03.1999 Bulletin 1999/09

(73) Proprietor: **Sony DADC Austria AG**
5081 Anif (AT)

(72) Inventors:
- **Blaukovitsch, Reinhard**
  5081 Anif (AU)
- **Winter, Andreas**
  5081 Anif (AU)

(74) Representative: **Müller, Frithjof E., Dipl.-Ing. et al**
Patentanwälte
MÜLLER & HOFFMANN,
Innere Wiener Strasse 17
81667 München (DE)

(56) References cited:
EP-A- 0 416 663
EP-A- 0 644 474
EP-A- 0 745 925
WO-A-98/03973
FR-A- 2 640 794
US-A- 5 538 773
US-A- 5 563 947
US-A- 5 659 613

- **"How disks are padlocked " IEEE SPECTRUM, vol. 23, no. 6, June 1986, NY, US, pages 32-40, XP002054317**

EP 0 899 733 B1

Description

[0001] The invention relates to the area of Compact Disc (CD) including all existing or future formats of CD Audio and CD-ROM and any existing or future combinations of compact discs or other optical storage media. In particular the present invention relates to a copy protection and to a copy control mechanism by authentication of optical record carriers, here to a method of obtaining a copy protected optical record carrier, a method of accessing a copy protected optical record carrier and such an optical record carrier itself.

[0002] Optical storage discs with information stored on one or both sides have come to be used for a variety of purposes, most notably in the music, games, video and computer industry. Digital information is stored on the optical storage media in the form of pits arranged along circular, concentric tracks on one or on both sides of the disc. The track is typically read from the inside out, but may also be read form outside in, as it is already used for some optical storage media. The data itself on the track is divided into sectors, each equal in length, containing equal amounts of information.

[0003] To manufacture an optical storage device, a CD glass master is made by exposing photoresist which is on a glass plate by a modulated laser. The modulation of the laser corresponds to the digital information that is stored on the final disc. Thereafter, exposure, developing and removing those exposed spots form tiny indentations in a single spiral on the glass master are conducted. The pattern and the length of the indentations along this track represent the recorded information digitally. Usually, in a following galvanic process nickel is applied to this glass master to get the nickel master which is the tool for moulding replicas in an injection moulding process. The pattern of the nickel master referred to as pits and land as illustrated in figure 1 is then embossed on the surface of a polycarbonate or PMMA substrate, which results in a copy of the nickel master that forms the basis of the optical storage disc. The stamped replicas are then coated with a reflective (aluminium or gold) layer and in order to prevent this reflective layer from oxidation a protective layer is applied to the discs.

[0004] Figure 2 illustrates the readout of a Compact Disc. A laser beam is focusing onto the surface of the disc. If the laser light falls on the land area most of it will be reflected. If the laser falls on a pit area the light will be refracted and scattered and only a small portion will return in the original direction. This means that the readout electronics can differ between a "0" or "NO" and a "1" or "YES" information and furthermore the electronics of a CD reader can reconstruct the digital information which was recorded onto the disc originally.

[0005] Although audio reproduction was the primary motivation for development of the CD, and because of cost reductions resulting from the popularity of audio CDs, the CD has recently become a preferred form for storing data for a computer in the form of read only memory, i.e. CD-ROM.

[0006] The format in which audio information is stored on a CD is known as the "Red Book" standard. Under Red Book digital data on a CD is organized into indexed tracks. As illustrated in figure 4, the digital samples for left and right audio channels are interleaved with error correcting codes, so called C1, C2 error corrections, and SUBCODE data into organized CD blocks. Throughout the disc, the interleaved SUBCODE information defines the current position in minutes, seconds, frames, both with respect to the current track and with respect to the entire disc.

[0007] The so called "Yellow Book" standard is typically as a format for a CD-ROM. The Yellow Book format is similar to the Red Book format in many respects, including the use of data organized into tracks, interleaved with error correction code and SUBCODE information but replacing the Audio information by computer data. Besides the Red Book and Yellow Book standard there exist many more standards developed for optical storage media covering audio data, computer data, video data and combinations of these information.

[0008] According to these standards every block of a CD has to be accessible.

[0009] Figure 3 illustrates a standard CD-ROM mode 1 data sector which consists of 12 bytes MAINCODE SYNCHRONIZATION FIELD, 3 bytes ADDRESS, 1 byte MODE, 2048 byte of USER DATA, 4 bytes ERROR DETECTION CODE, 8 bytes of ZEROS and 276 bytes of ERROR CORRECTION CODE. Such a CD-ROM data sector, i.e. CD block or block, comprises 2352 bytes and is 1/75 (one seventy-fifth) of a second.

[0010] The 2352 bytes of 1 data sector are carried in 98 Frames depicted in figure 4, wherein each Frame includes 24 bytes of said data sector. Additionally to this data, each Frame comprises 4 bytes C2 error correction, 4 bytes CI error correction and 1 byte SUBCODE data. The 1 byte SUBCODE data is divided into 8 SUBCODE channels called SUBCODE P, Q, R, S, T, U, V, W field, which are also shown in figure 4. Each SUBCODE channel consists of 98 bits that are build by 2 synchronization bits and 96 data bits,

[0011] As is illustrated in figure 5, a SUBCODE Q channel consists of 98 bits, which is referred to as SUBCODE Q field in this invention. All other SUBCODE channels (P, R, S, T, U, V, W) are similar to the Q channel, but carry different information. The first 2 bits of each SUBCODE channel represent the SUBCODE SYNC patterns SO and S1. These patterns are necessary to synchronize a CD reader to spin the CD at a constant linear velocity.

[0012] Each SUBCODE channel has a different function and content, the following description refers to the SUBCODE Q channel only.

[0013] The next 4 bits after the SUBCODE SYNC patterns represent the CONTROL FIELD which describes the kind

of information of a track as shown in table 1.

Table 1:

SUBCODE Q CONTROL FIELD	
MSB	LSB
00x0	2 audio channels without pre-emphasis
00x1	2 audio channels with pre-emphasis of 50/15 μseconds
10x0	4 audio channels without pre-emphasis
00x1	4 audio channels with pre-emphasis of 60/15 μ seconds
01x0	data track (CD-ROM)
01x1	reserved
11xx	reserved
xx0x	digital copy prohibited
xx1x	digital copy permitted

The next four bits represent the ADDRESS FIELD and specify the mode. There are several modes (e.g. mode 1, mode 2, mode 3) but for the background of this invention the address mode 1 is explained in detail only.

[0014] For mode 1 there are two different data formats possible. For the background of this invention an explanation of the program and lead-out area only of the SUBCODE Q channel is given, as it is illustrated in figure 5.

[0015] TNO, 8 bits, represents the track number running from 0 to 99. A track numbered with AA represents the lead-out track.

[0016] X, 8 bits, represents the index number within a track which can range between 0 to 99.

[0017] MIN, SEC, FRAME, 8 bits each, is the running time within a track expressed in 6 digits BCD, The minutes of a track are stored in MIN, the seconds are stored in SEC and the frames are stored in FRAME. One second is subdivided into 75 frames (from 0 to 74).

[0018] ZERO, all 8 bits are set to zero (0x00).

[0019] AMIN, ASEC, AFRAME, 8 bits each, is the running time on the disc expressed in 6 digits BCD. The minutes of a track are stored in AMIN, the seconds are stored in ASEC and the frames are stored in AFRAME. One second is subdivided into 75 frames (from 0 to 74).

[0020] CRC is a 16 bit cyclic redundancy check on CONTROL, ADDRESS, TNO, X, MIN, SEC, FRAME, ZERO, AMIN, ASEC, and AFRAME. On the disc the parity bits are inverted. The remainder has to be checked at zero. The CRC is calculated according to following polynomial:

$$P(x) = x^{16} + x^{12} + x^5 + 1$$

[0021] The 16 bit CRC field is a parity information that checks the correctness of the CONTROL, ADDRESS, TNO, X, MIN, SEC, FRAME, ZERO, AMIN, ASEC, and AFRAME fields.

[0022] Despite apparent advantages of CD-ROM there remain some drawbacks to use a compact disc for marketing and selling large and expensive software packages. A serious drawback is that there is currently no reliable method of protecting a CD-ROM from being copied. The content of a CD-ROM nowadays can be copied onto a hard disc drive or directly onto a CD-Recordable, i.e. CD-R. The software packages illegally copied on a CD-R or on a hard disc drive of a computer will again work without any technical problems.

[0023] EP 0 745 925 A2 describes a system and method for encrypting and decrypting encoded data wherein a randomly accessible removeable storage element such as a diskette carries an encryption key which corresponds to a pattern of physically marked sectors on said storage element. The marked sectors are identified by evaluating that data retrieved therefrom is invalid.

[0024] WO 98/03973 A2 which is a document according to Art. 158(1) and 54(3) EPC discloses to provide an improved protection against undesired or illegal copying by giving different than linearly increasing address values to address labels of at least one specific sector. Since a standard optical recording apparatus can not create such address labels, but only linearly increasing address values, dependent upon a verification of such an address value an optical disc playback apparatus aborts the playback. Furthermore, also copying can be aborted in case an optical disc recording apparatus receives such an address value.

[0025] Therefore, it is an object of the present invention to provide a method of preventing copies of original optical record carriers to be made, in particular a method of creating a key on an original optical record carrier which cannot

be copied onto another data carrier and a method of extracting that key off the original optical record carrier in order to be able to distinguish between an original optical record carrier and a copied optical record carrier. Further, it is an object of the present invention to provide an optical record carrier that has a secure copy protection.

[0026] The method of obtaining a copy protected optical record carrier carrying information in different blocks according to the invention comprises the following steps:

(a) define number and addresses of blocks used for copy protection;
(b) convert number and addresses selected in step (a) into a copy protection key;
(c) encrypt information data to be recorded onto the record carrier with copy protection key obtained in step (b); and is characterized by the following steps:
(d) create a master having subcode fields which are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards for blocks selected in step (a) and encrypted information data in other blocks; and
(e) replicate record carrier with master created in step (d).

[0027] The method of accessing a copy protected optical record carrier carrying information in different blocks wherein data is retrieved from the record carrier and decrypted with a copy protection key according to the invention comprises the following steps:

(a) find blocks having correponding subcode fields which subcode fields are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards; and
(b) extract a copy protection key from number and addresses of said blocks having a modified correponding subcode field found in step (a) to decrypt the retrieved data therewith.

[0028] The optical record carrier carrying information in different blocks according to the invention is characterized in that subcode fields of a predetermined number of individual accessible blocks with a respective predetermined address are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards, and the record carrier contains information data encrypted with a copy protection key defined by the number and addresses of the blocks having said modified subcode fields.

[0029] Preferred embodiments of the invention are defined in the respective subclaims dependent on the independent claims 1, 8 and 15.

[0030] An embodiment of the present invention concerns a method of creating compact discs that carry a unique identifier, which can also be named as key or fingerprint, since this unique identifier is realized by generating blocks that have modified subcode fields in a predetermined pattern. This method is applicable to mass production. In a further embodiment, a method is described of how to retrieve this identifier and a computer equipped with a CD-ROM drive.

[0031] Any data can be stored on the optical storage media, the present invention does not require special data to be recorded nor is there any limitation in the amount of the data in regard to this invention.

[0032] In a preferred embodiment, the fingerprint or key of the compact disc is incorporated by implementing a certain amount of SUBCODE Q field modifications throughout the program area of the disc. These SUBCODE Q field modifications result in invalid SUBCODE Q fields. On the other hand, a CD block corresponding to an invalid SUBCODE Q field is still accessible, since its address is also stored in the main code header, as it is shown in figure 5.

[0033] According to another aspect, the present invention is applicable to a method of encrypting at least one part of a main application or data files stored on a compact disc and the decryption of this at least one encrypted part after retrieving the correct fingerprint of the compact disc by using the copy protection key as the decryption tool.

[0034] According to a further aspect, the present invention can be used to implement one or more keys on a compact disc in form of various SUBCODE Q field modification patterns.

[0035] The main advantage for a user is that no keys have to be entered during the authentication process of the copy protected record carrier, as the predetermined pattern of blocks with modified subcode information is known before the manufacturing and can be implemented in the data included on the respective record carrier. In combination with external keys, that have to be entered during the access procedure, e.g. by the user, for example also only parts of the content of a compact disc can be unlocked from an original disc. This feature allows the possibility of creating multiple language versions or more or less enhanced versions of a software package which can be restored off an original disc only by "pay for unlock".

[0036] This invention is not restricted to any specific format of the wide variety of optical storage media, i.e. audio data, computer data, video data or combinations therefrom, it is rather applicable to all existing optical storage media formats.

[0037] As will be shown in the following detailed description of the present invention, CD readers return different results when retrieving sectors, i.e. blocks, which correspond to valid or invalid SUBCODE Q fields. Based on those

differences the extracted key will be utilized to descramble or decrypt those parts of the main application that have been encrypted before. If the decryption was done with the correct key upon retrieving it from an original disc, or in other words, it the decryption was done with the same key that has been used for encrypting the application beforehand, the main application can be fully restored to its generic layout and will properly work on the computer platform that it was designed for. Since the SUBCODE Q fields are normally not directly copied from one disc to another, as the main code data, but are newly generated during the copy process, retrieving a key from a copied or non original disc will result in a different key than the one that has been used for encrypting, and will furthermore result in a different decryption process and decryption result. Therefore it is not possible to execute such a decrypted application on the computer platform that it was designed for.

[0038] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and, together with a general description of the invention given above, and the detailed description of the embodiment given below, serve to explain the principles of the invention, wherein:

Figure 1 illustrates the pattern of the nickel master referred to as pits and land which is then embossed on the surface of a polycarbonate or PMMA substrate.
Figure 2 illustrates the readout of a Compact Disc;
Figure 3 illustrates a standard CD-ROM mode 1 data sector;
Figure 4 illustrates the structure of CD-ROM data encoded on a Compact Disc, which consists of data, C1, C2 error correction and 8 SUBCODE channels called SUBCODE P, Q. R, S, T, U, V, W;
Figure 5 illustrates the detailed layout of 98 bits of the SUBCODE Q channel;
Figure 6 is a chart of the distribution of resumed SUBCODE Q fields by CD-ROM drives when seeking for an invalid SUBCODE Q field;
Figure 7 is a chart of the distribution of returned SUBCODE Q fields by CD-ROM drives when seeking for a valid SUBCODE Q field;
Figure 8 is a flow chart of the encoding and manufacturing process of copy protected compact disc by subcode Q field modifications; and
Figure 9 is a flow chart of the operations performed by a protected application and protected disc when used in a computer system.

[0039] In the following, a method of creating a unique key on optical storage media, e.g. compact discs, and the method of extracting or reading this fingerprint off the disc is described.

[0040] As stated above, the main data of each CD-ROM sector is associated to a SUBCODE Q channel or SUBCODE Q field which contains the unique address (in minutes, seconds, frames) of this sector. A 60 minute CD-ROM e.g. contains 270 000 sectors and 270 000 SUBCODE Q fields.

[0041] Since the SUBCODE Q fields normally will be regenerated during the copy process, a predetermined pattern of invalid SUBCODE g fields, e.g. SUBCODE Q fields carrying invalid addresses, can serve as unique identifier of the disc itself. As stated above, a disc accessing device, e.g. a CD-ROM reader, can distinguish between a block with invalid SUBCODE Q field and a block having a valid SUBCODE Q field, e.g. a SUBCODE Q field carrying a valid address, therefore, when accessing such a block having an invalid SUBCODE Q field, the accessing device first resumes a wrong block. On the other hand, there is no possibility to produce a defect SUBCODE Q field for a device that facilitates the production of an optical disc, since the SUBCODE Q field is not directly copied onto the disc from the original, but newly generated during the copy process. Therefore, an illegal copy contains only valid SUBCODE Q fields, which makes it possible to distinguish between an original and a copied product.

[0042] Since the address of a block is not only stored in the corresponding SUBCODE Q field, but also in the main code header, as shown in figure 5, an optical disc comprising invalid SUBCODE Q fields is still within the standard, e. g. the Yellow Book for CD-ROM, since all blocks can be accessed at least with the help of their address stored in the main code header.

[0043] When a CD-ROM drive is reading any sector on a compact disc, typically the drive scans along the track and decodes the SUBCODE Q addresses. Once getting close to the address that has been sought for, the firmware of the drive decodes the address in the main code header and returns this sector to the calling application.

[0044] There is also the possibility of getting the position of the optical pickup of a CD-ROM reader by seeking for a certain address and asking the drive for the position of the pick up. Before returning the SUBCODE Q field to the calling application the firmware of the drive recalculates the SUBCODE Q CRC field and validates the content of the remaining bytes in the SUBCODE Q field. If the checked SUBCODE Q field was free of error the drive will return the SUBCODE Q field that it has been asked for. If the recalculation of the 16 CRC bits results in a mismatch to the stored 16 bits CRC on the disc, the drive will not return the SUBCODE Q field that it has been asked for. Depending on the strategy of the drive, it will return the content of the SUBCODE Q fields of one or more blocks before or after the block which contained an error in the SUBCODE Q field, i.e. an invalid SUBCODE Q field.

[0045] The search for the SUBCODE Q field modifications on the compact disc can be conducted by a special device or by a software tool. In an embodiment of this invention a program seeks for certain addresses including at least all those that have been set invalid by implementing a modification on the SUBCODE Q field during the mastering process. Depending on the strategy of the CD-ROM reader it will return a SUBCODE Q field that is either one or more blocks before or after the block that contains the error when trying to access a block having an invalid address in the corresponding SUBCODE Q field.

[0046] Figure 6 illustrates the distribution of resumed blocks of a variety of CD-ROM drives when accessing a SUBCODE Q field that contains an error. Here, a Gaussian distribution around the invalid SUBCODE Q field is shown that has a gap at the position of the invalid SUBCODE Q field.

[0047] Figure 7, on the other hand, demonstrates the distribution of resumed blocks of a variety of CD-ROM drives when accessing a SUBCODE Q field when there is no error in this field. Here, a Gaussian distribution around the invalid SUBCODE Q field is shown that has no gap at the position of the invalid SUBCODE Q field.

[0048] As can be seen in figure 6 and figure 7 there is a difference in the return values of CD-ROM drives when seeking for an invalid SUBCODE Q field or when seeking for a valid SUBCODE Q field. This difference in the return values and furthermore the location of the difference results in the key that is then extracted of the optical disc.

[0049] Figure 8 shows a flowchart of an encoding and manufacturing process of copy protected compact discs according to the invention.

[0050] After starting the process in step S1, a certain number of SUBCODE Q fields and corresponding addresses are freely defined in step S2. These SUBCODE Q fields form the unique identifier of all valid record carriers of this type. These defined SUBCODE Q fields lateron undergo a SUBCODE Q field modification. which furthermore respectively results in an invalid SUBCODE Q field. A typical range of modified SUBCODE Q fields in an embodiment of this invention runs between a number of 6 and 60. The creation of these modifications is realized in the mastering stage. As alternative, a software programme that generates the SUBCODE frames also creates those SUBCODE Q field modifications as predefined.

[0051] In a following step S3 the addresses of the SUBCODE Q fields selected in step S2 are converted into a copy protection key. Using this key, the data to be stored on the disc, e.g. an application programme or user data, is encrypted in step S4. Thereafter, in step S5, an extraction and decryption programme will be appended to the encrypted data, to allow the user to access the data without any) special requirements. The extraction programme scans the disc at least for invalid SUBCODE Q fields and extracts the copy protection key therefrom. Of course, it is also possible that the copy protection key is based on a combination of valid and invalid SUBCODE Q fields. The decryption programme decrypts the accessed data using the extracted copy protection key.

[0052] During the mastering process in step S6, when exposing the photoresist by the laser that is modulated by the data, all SUBCODE Q field modifications will be placed on the glass master.

[0053] Therefore, in step S7, each CD that is embossed in the replication process by such a created stamper carries exactly the same SUBCODE Q field modifications. Since the number and also the addresses of the invalid SUBCODE Q fields are known before manufacturing of the disc, i.e. of the glass master, and can be incorporated into the data stored on the disc, the SUBCODE Q filed modifications, i.e. the invalid SUBCODE Q fields, can be taken as the key or the fingerprint that the CDs have been provided with. The data stored on the disc can then only be accessed if the key stored on the disc as data matches to the key included on the disc on the basis of invalid SUBCODE Q fields or if the data stored on the disc is decrypted using the copy protection key extracted from the disc.

[0054] The encryption of an application that this copy protection system is used for can be any standard method. A variety of encrypting schemes and methods exists, such as byte substitution, word substitution or polynomial functions by two byte-arrays, whereas the first byte-array represents the user application and the second byte-array represents the key. The application can be encrypted completely or just partially. If partial encryption has been chosen typically 4 to 2048 bytes are encrypted. Also several different encryption schemes or keys can be used for different parts of the application stored on the optical storage medium.

[0055] Figure 9 shows a flow chart of the operations performed by a protected application and a protected disc when used in a computer system.

[0056] After the start of the process in step S10, the insertion of a copy protected disc into the CD-ROM drive in step S11 and the starting of the encrypted application in step S12, the process is set forth with the extracting procedure.

[0057] First, in step S13 a search for at least predetermined invalid SUBCODE Q fields is conducted. According to an embodiment of this invention, a predetermined number of blocks having predetermined addresses will be checked for valid or invalid SUBCODE Q fields. Depending on the returned results from the CD-ROM drive it is validated if a predetermined block is directly accessible or not. A list of these results will be stored. This list comprises all of these predetermined blocks and the respective corresponding result.

[0058] Once the scanning for predetermined SUBCODE Q fields has been completed the copy protection key will be extracted in step S14 according to the list stored in step S13. Upon extracting at least predetermined invalid SUBCODE Q fields the fingerprint or the unique key of the optical disc can be regenerated. This key was originally taken

to partially or completely encrypt the application.

[0059] Now this key is taken to decrypt the encrypted application in step S15. If it is determined in step S16 that the original key and the extracted key match, the decryption will work properly and the application can be loaded and run in step S17. On the other hand, if the extraction of the key was done off a non original disc, the extraction will result in a different key than the original key. Therefore, a decryption of an application by utilising a non original key will result in a non workable application and the process will stop in step S18.

Claims

1. Method of obtaining a copy protected optical record carrier carrying information in different blocks, comprising the following steps:

   (a) define number and addresses of blocks used for copy protection (S2);
   (b) convert number and addresses selected in step (a) into a copy protection key (S3);
   (c) encrypt information data to be recorded onto the record carrier with copy protection key obtained in step (b) (S4); **characterized by** the following steps:
   (d) create a master having subcode fields which are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards for blocks selected in step (a) and encrypted information data in other blocks (S6); and
   (e) replicate record carrier with master created in step (d) (S7).

2. Method according to claim 1, **characterized in that** said step (c) of encrypting information data additionally comprises the following step: append extraction and decryption programme to said encrypted data (S5), wherein said extraction programme finds said blocks carrying modified subcode information and extracts said copy protection key therefrom, and said decryption programme decrypts said encrypted information data according to said copy protection key extracted by said extraction programme when they are executed.

3. Method according to anyone of claims 1 to 2, **characterized in that** said modified subcode fields are modified as to be recognized invalid by a reading device.

4. Method according to anyone of claims 1 to 3, **characterized in that** said modified subcode fields are created so that they include no or invalid address information.

5. Method according to anyone of claims 1 to 4, **characterized in that** said modified subcode fields are SUBCODE Q fields.

6. Method according to anyone of claims 1 to 5, **characterized in that** said record carrier is a compact disc and said information is audio data together with control data and information data.

7. Method according to anyone of claims 1 to 5, **characterized in that** said record carrier is a compact disc read only memory and said information is any form of digital data.

8. Method of accessing a copy protected optical record carrier carrying information in different blocks wherein data is retrieved from the record carrier and decrypted with a copy protection key, **characterized by** the following steps:

   (a) find blocks having correponding subcode fields which subcode fields are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards (S13); and
   (b) extract a copy protection key from number and addresses of said blocks having a modified correponding subcode field found in step (a) (S14) to decrypt the retrieved data therewith (S15).

9. Method according to claim 8, **characterized in that** said step (a) includes the finding of blocks having a modified correponding SUBCODE Q field.

10. Method according to claim 9, **characterized in that** said step (a) includes the following steps:

    (a1) trying to access a predetermined block based on the address defined in the SUBCODE Q field of said block by sending a respective command to an optical pickup of a disc drive to access said predetermined block;

(a2) determining if said optical pickup has accessed said predetermined block by checking of the block address defined in the SUBCODE Q field or the main code data directly after the access procedure of the optical pickup; and
(a3) storing all block addresses of blocks the optical pickup could not access directly.

11. Method according to claim 10, **characterized in that** said step (a3) additionally comprises the step of storing all block addresses of blocks the optical pickup could access directly, and in said step (b) of extracting a copy protection key said key is extracted from a pattern of said blocks having a modified correponding subcode field and of said blocks having no modified correponding subcode field.

12. Method according to anyone of claims 8 to 11, **characterized in that** said step of retrieving data from the record carrier comprises the following steps:

comparison of the copy protection key extracted in step (b) and a copy protection key appended to the information carried by the record carrier;
allowing at least partial or no access to said information data in dependency on the correlation of said both copy protection keys.

13. Method according to anyone of claims 8 to 12, **characterized in that** said step of retrieving data from the record carrier comprises the following steps:

comparison of a copy protection key entered during the data retrieval with the copy protection key extracted in step (b), and
allowing at least partial or no access to said information data in dependency on the correlation of said both copy protection keys.

14. Method according to anyone of claims 8 to 13, **characterized in that** said steps of data retrieval are conducted with the help of software included on the record carrier.

15. Optical record carrier carrying information in different blocks, **characterized in that**

subcode fields of a predetermined number of individual accessible blocks with a respective predetermined address are respectively modified in respect to the CD "Red Book" or the CD-ROM "Yellow Book" standards, and
the record carrier contains Information data encrypted with a copy protection key defined by the number and addresses of the blocks having said modified Subcode fields.

16. Record carrier according to claim 15, **characterized in that** said modifled subcode fields are invalid.

17. Record carrier according to anyone of claims 15 or 16, **characterized in that** said modified subcode fields are SUBCODE Q fields.

18. Record carrier according to anyone of claims 15 to 17, **characterized in that** said record carrier is a compact disc and said information is audio data together with control data and information data.

19. Record carrier according to anyone of claims 15 to 17, **characterized in that** said record carrier is a compact disc read only memory and said information is any form of digital data.

Patentansprüche

1. Verfahren zur Erzeugung eines kopiergeschützten optischen Aufzeichnungsträgers, der Information in verschiedenen Blöcken speichert, umfassend die folgenden Schritte:

(a) Definition der Anzahl und der Adressen von für den Kopierschutz verwendeten Blöcken (S2);
(b) Konvertierung der im Schritt (a) ausgewählten Anzahl und Adressen in einen Kopierschutzschlüssel (S3);
(c) Verschlüsseln der auf dem Aufzeichnungsträger aufzunehmenden Informationsdaten mit dem im Schritt (b) erhaltenen Kopierschutzschlüssel (S4); **gekennzeichnet durch** die folgenden Schritte:

(d) Erzeugung eines Masters mit Subcodefeldern, die jeweils hinsichtlich des "Red Book" Standards für CDs oder des "Yellow Book" Standards für CD-ROMs modifiziert sind, bei im Schritt (a) ausgewählten Blöcken und verschlüsselten Informationsdaten in anderen Blöcken (S6); und
(e) Replikation eines Aufzeichnungsträgers mit dem im Schritt (d) erzeugten Master (S7).

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß der Schritt (c) des Verschlüsselns der Informationsdaten zusätzlich den folgenden Schritt umfasst:
Anfügen eines Extraktionsprogramms und eines Entschlüsselungsprogramms an die verschlüsselten Daten (S5), wobei das Extraktionsprogramm die Blöcke mit modifizierter Subcodeinformation findet und daraus den Kopierschutzschlüssel extrahiert, und das Entschlüsselungsprogramm die verschlüsselten Daten bei ihrer Ausführung entsprechend des durch das Extraktionsprogramm extrahierten Kopierschutzschlüssels entschlüsselt.

3. Verfahren nach einem der Ansprüche 1 bis 2, **dadurch gekennzeichnet**, daß die modifizierten Subcodefelder so modifiziert sind, daß sie von einer Lesevorrichtung als ungültig erkannt werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß die modifizierten Subcodefelder so erzeugt sind, daß sie keine oder ungültige Adresseninformation enthalten.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet** daß die modifizierten Subcodefelder SUBCODE Q Felder sind.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß der Aufzeichnungsträger eine Compactdisc (CD) ist und die Information aus Audiodaten zusammen mit Steuerdaten und Informationsdaten besteht.

7. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß der Aufzeichnungsträger ein Compactdisc-Nur-Lese-Speicher (CD-ROM) ist und die Information aus einer beliebigen Form digitaler Daten besteht.

8. Verfahren des Zugriffs auf einen kopiergeschützten optischen Aufzeichnungsträger, der Information in verschiedenen Blöcken speichert, bei dem Daten von dem Aufzeichnungsträger wiedergewonnen und mit einem Kopierschutzschlüssel entschlüsselt werden, **gekennzeichnet durch** die folgenden Schritte:

(a) Finden von Blöcken mit korrespondierenden Subcodefeldern, die jeweils hinsichtlich des "Red Book" Standards für CDs oder des "Yellow Book" Standards für CD-ROMs modifiziert sind (S13); und
(b) Extrahieren eines Kopierschutzschlüssels aus Anzahl und Adressen der im Schritt (a) gefundenen Blöcke mit einem modifizierten korrespondierenden Subcodefeld (S14), um die wiedergewonnenen Daten damit zu entschlüsseln (S15).

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet**, daß der Schritt (a) das Finden von Blöcken mit einem modifizierten korrespondierenden SUBCODE Q Feld enthält.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet**, daß der Schritt (a) die folgenden Schritte enthält:

(a1) Versuch des Zugriffs auf einen bestimmten Block auf Grundlage der in dem SUBCODE Q Feld des Blocks definierten Adresse durch das Senden eines entsprechenden Befehls an einen optischen Aufnehmer eines Plattenlaufwerks, auf den bestimmten Block zuzugreifen;
(a2) Überprüfung, ob der optische Aufnehmer auf den bestimmten Block zugegriffen hat, indem die in dem SUBCODE Q Feld definierte Blockadresse oder die Hauptcodedaten direkt nach dem Zugriffsverfahren des optischen Aufnehmers überprüft werden; und
(a3) Speichern aller Blockadressen der Blöcke, auf die der optische Aufnehmer nicht direkt zugreifen konnte.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet**, daß der Schritt (a3) zusätzlich den Schritt des Speicherns aller Blockadressen der Blökke enthält, auf die der optische Aufnehmer direkt zugreifen könnte, und in dem Schritt (b) der Extraktion eines Kopierschutzschlüssels der Schlüssel aus einem Muster der Blöcke mit einem modifizierten korrespondierenden Subcodefeld und der Blöcke mit keinem modifizierten korrespondierenden Subcodefeld extrahiert wird.

12. Verfahren nach einem der Ansprüche 8 bis 11, **dadurch gekennzeichnet**, daß der Schritt der Wiedergewinnung von Daten von dem Aufzeichnungsträger die folgenden Schritte umfaßt:

Vergleich des im Schritt (b) extrahierten Kopierschutzschlüssels und eines an die auf dem Aufzeichnungsträger gespeicherte Information angefügten Kopierschutzschlüssels;
Erlauben eines wenigstens teilweisen oder keines Zugriffs auf die Informationsdaten in Abhängigkeit der Korrelation der beiden Kopierschutzschlüssel.

13. Verfahren nach einem der Ansprüche 8 bis 12, **dadurch gekennzeichnet**, daß der Schritt der Wiedergewinnung von Daten von dem Aufzeichnungsträger die folgenden Schritte umfaßt:

Vergleich eines während der Datenwiedergewinnung eingegebenen Kopierschutzschlüssels mit dem im Schritt (b) extrahierten Kopierschutzschlüssel, und
Erlauben eines wenigstens teilweisen oder keines Zugriffs auf die Informationsdaten in Abhängigkeit der Korrelation der beiden Kopierschutzschlüssel.

14. Verfahren nach einem der Ansprüche 8 bis 13, **dadurch gekennzeichnet**, daß die Schritte der Datenwiedererlangung mit Hilfe von auf dem Aufzeichnungsträger enthaltener Software durchgeführt werden.

15. Optischer Aufzeichnungsträger, der Informationen in unterschiedlichen Blöcken speichert, **dadurch gekennzeichnet**, daß

Subcodefelder einer bestimmten Anzahl individuell zugreifbarer Blökke mit einer jeweiligen bestimmten Adresse jeweils hinsichtlich des "Red Book" Standards für CDs oder des "Yellow Book" Standards für CD-ROMs modifiziert sind, und
der Aufzeichnungsträger mit einem durch die Anzahl und Adressen der Blöcke mit den modifizierten Subcodefeldern definierten Kopierschutzschlüssel verschlüsselte Informationsdaten enthält.

16. Aufzeichnungsträger nach Anspruch 15, **dadurch gekennzeichnet**, daß die modifizierten Subcodefelder ungültig sind.

17. Aufzeichnungsträger nach einem der Ansprüche 15 oder 16, **dadurch gekennzeichnet**, daß die modifizierten Subcodefelder SUBCODE Q Felder sind.

18. Aufzeichnungsträger nach einem der Ansprüche 15 bis 17, **dadurch gekennzeichnet**, daß der Aufzeichnungsträger eine Compactdisc (CD) ist und die Information aus Audiodaten zusammen mit Steuerdaten und Informationsdaten besteht.

19. Aufzeichnungsträger nach einem der Ansprüche 15 bis 17, **dadurch gekennzeichnet**, daß der Aufzeichnungsträger ein Compactdisc-Nur-Lese-Speicher (CD-ROM) ist und die Information aus einer beliebigen Form digitaler Daten besteht.

Revendications

1. Procédé d'obtention d'un support d'enregistrement optique protégé en copie qui porte des informations dans des blocs différents, le procédé comprenant les opérations suivantes:

(a) définir un nombre et des adresses de blocs utilisés pour la protection en copie (S2) ;
(b) convertir le nombre et les adresses sélectionnés lors de l'opération (a) en un code de protection en copie (S3);
(c) crypter des données d'informations devant être enregistrées sur le support d'enregistrement au moyen du code de protection en copie obtenu lors de l'opération (b) (S4);
caractérisé par les opérations suivantes :
(d) créer un disque "père" comportant des zones de sous-codes qui sont respectivement modifiées relativement aux normes "Livre rouge (ou Red Book)" pour disques audio numériques de format compact (notés CD) ou "Livre jaune (ou Yellow Book)" pour mémoires mortes sur CD (notées CD-ROM) pour les blocs sélectionnés lors de l'opération (a) et les données d'informations cryptées se trouvant dans d'autres blocs (S6) ; et
(e) reproduire un support d'informations au moyen du disque père créé lors de l'opération (d) (S7).

2. Procédé selon la revendication 1, caractérisé en ce que l'opération (c) de cryptage de données d'informations

comprend en outre l'opération suivante:

ajouter des programmes d'extraction et de décryptage auxdites données cryptées (S5), où ledit programme d'extraction recherche lesdits blocs portant des informations de sous-codes modifiées et en extrait ledit code de protection en copie, et ledit programme de décryptage décrypte lesdites données d'informations cryptées en fonction dudit code de protection en copie qui a été extrait par ledit programme d'extraction, lorsqu'ils sont exécutés.

3. Procédé selon l'une quelconque des revendications 1 et 2, caractérisé en ce que lesdites zones de sous-codes modifiées sont modifiées de façon à être reconnues comme non valables par un dispositif de lecture.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que lesdites zones de sous-codes modifiées sont créées de façon qu'elles ne comportent aucune information d'adresse ou qu'elles comportent une information d'adresse non valable.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que lesdites zones de sous-codes modifiées sont des zones de SOUS-CODES Q.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit support d'enregistrement est un disque de format compact et en ce que lesdites informations sont des données audio ainsi que des données de commande et des données d'informations.

7. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit support d'enregistrement est une mémoire morte sur disque de format compact et lesdites informations sont des données numériques se présentant sous une forme quelconque.

8. Procédé d'accession à un support d'enregistrement optique protégé en copie qui porte des informations dans des blocs différents, où les données sont extraites du support d'enregistrement et sont décryptées au moyen d'un code de protection en copie, le procédé étant caractérisé par les opérations suivantes:

(a) rechercher des blocs qui possèdent des zones de sous-codes correspondantes, lesquelles zones de sous-codes sont respectivement modifiées en relation avec les normes et "Livre rouge (ou Red Book)" pour disques audio numériques de format compact (notés CD) ou "Livre jaune (ou Yellow Book)" pour mémoires mortes sur CD (notées CD-ROM) (S 13) ; et
(b) extraire un code de protection en copie à partir d'un nombre et d'adresses desdits blocs ayant une zone de sous-code correspondante modifiée que l'on a trouvés lors de l'opération (a) (S14) afin de décrypter les données extraites au moyen de celui-ci (S 15).

9. Procédé selon la revendication 8, caractérisé en ce que ladite opération (a) comporte la recherche de blocs ayant une zone de SOUS-CODE Q correspondante modifiée.

10. Procédé selon la revendication 9, caractérisé en ce que ladite opération (a) comporte les opérations suivantes:

(a1) essayer de faire accès à un bloc prédéterminé sur la base de l'adresse définie dans la zone de SOUS-CODE Q dudit bloc en envoyant une instruction respective à une tête de lecture optique d'une unité de lecture de disque afin de faire accès audit bloc prédéterminé ;
(a2) déterminer si ladite tête de lecture optique a fait accès audit bloc prédéterminé en contrôlant l'adresse de bloc définie dans la zone SOUS-CODE Q ou les données de code principales directement après la procédure d'accès faite par la tête de lecture optique ; et
(a3) stocker toutes les adresses de blocs auxquelles la tête de lecture optique ne pourrait pas faire accès directement.

11. Procédé selon la revendication 10, caractérisé en ce que ladite opération (a3) comprend en outre l'opération consistant à stocker toutes les adresses de blocs auxquelles la tête de lecture optique pourrait faire accès directement, et, lors de ladite opération (b) d'extraction d'un code de protection en copie, ledit code est extrait d'une configuration desdits blocs ayant une zone de sous-code correspondante modifiée et desdits blocs n'ayant aucune zone de sous-code correspondante modifiée.

12. Procédé selon l'une quelconque des revendications 8 à 11, caractérisé en ce que ladite opération consistant à extraire des données dudit support d'enregistrement comprend les opérations suivantes:

comparer le code de protection en copie extrait lors de l'opération (b) et un code de protection en copie qui a été ajouté aux informations portées par le support d'enregistrement ;
permettre un accès au moins partiel ou ne permettre aucun accès auxdites données d'informations en fonction de la corrélation entre lesdits deux codes de protection en copie.

13. Procédé selon l'une quelconque des revendications 8 à 12, caractérisé en ce que ladite opération consistant à extraire des données du support d'enregistrement comprend les opérations suivantes:

comparer un code de protection en copie qui a été introduit pendant l'extraction de données avec le code de protection en copie qui a été extrait lors de l'opération (b), et
permettre un accès au moins partiel ou ne permettre aucun accès auxdites données d'informations en fonction de la corrélation entre lesdits deux codes de protection en copie.

14. Procédé selon l'une quelconque des revendications 8 à 13, caractérisé en ce que l'on effectue lesdites opérations d'extraction de données à l'aide d'un logiciel inclus dans le support d'enregistrement.

15. Support d'enregistrement optique portant des informations dans des blocs différents, caractérisé en ce que:

des zones de sous-code d'un nombre prédéterminé de blocs accessibles distincts ayant une adresse prédéterminée respective sont respectivement modifiées relativement aux normes "Livre rouge (ou Red Book)" pour disques audio numériques de format compact (notés CD) ou "Livre jaune (ou Yellow Book)" pour mémoires mortes sur CD (notées CD-ROM), et
le support d'enregistrement contient des données d'informations cryptées au moyen d'un code de protection en copie qui est défini par le nombre et les adresses des blocs ayant lesdites zones de sous-codes modifiées.

16. Support d'enregistrement selon la revendication 15, caractérisé en ce que lesdites zones de sous-codes modifiées sont non valables.

17. Support d'enregistrement selon l'une quelconque des revendications 15 et 16, caractérisé en ce que lesdites zones de sous-codes modifiées sont des zones de SOUS-CODES Q.

18. Support d'enregistrement selon l'une quelconque des revendications 15 à 17, caractérisé en ce que ledit support d'enregistrement est un disque de format compact et en ce que lesdites informations sont des données audio ainsi que des données de commande et des données d'informations.

19. Support d'enregistrement selon l'une quelconque des revendications 15 à 17, caractérisé en ce que ledit support d'enregistrement est une mémoire morte sur disque de format compact et lesdites informations sont des données numériques se présentant sous une forme quelconque.

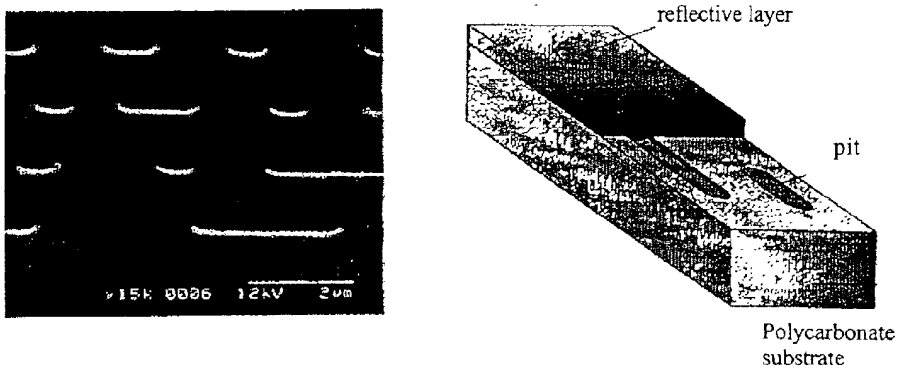

Fig. 1

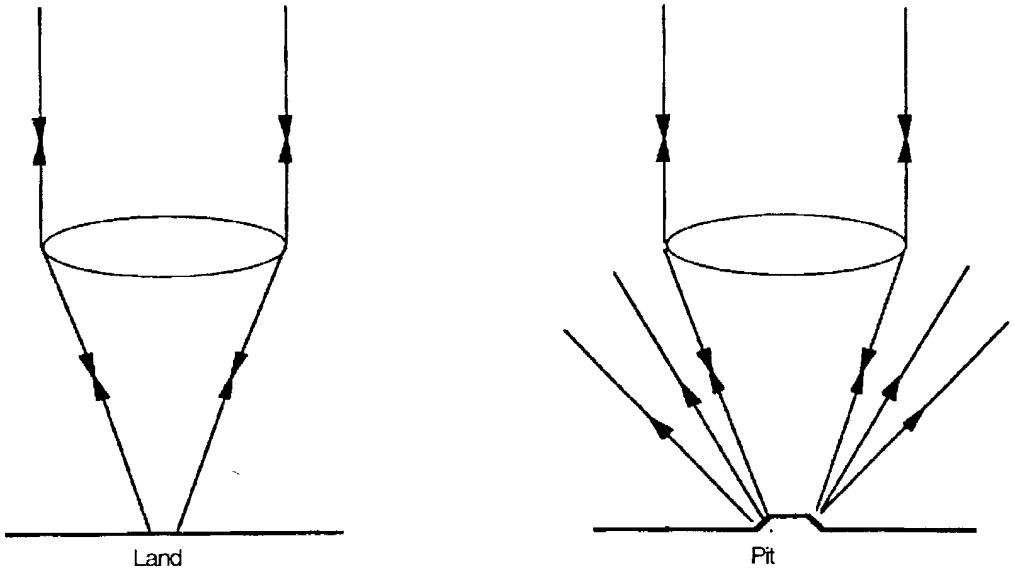

Fig. 2

Sync (12)	Header (4)				User data (2048)	Auxiliary data			
	min	sec	frame	mode		EDC (4)	Zero (8)	ECC (276)	
								P - Parity (172)	Q - Parity (104)

Fig. 3

Frame 0	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	Synchronization
Frame 1	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	Synchronization
Frame 2	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_0 Q_0 R_0 S_0 T_0 U_0 V_0 W_0
Frame 3	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_1 Q_1 R_1 S_1 T_1 U_1 V_1 W_1
Frame 4	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_2 Q_2 R_2 S_2 T_2 U_2 V_2 W_2
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
Frame 95	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_{93} Q_{93} R_{93} S_{93} T_{93} U_{93} V_{93} W_{93}
Frame 96	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_{94} Q_{94} R_{94} S_{94} T_{94} U_{94} V_{94} W_{94}
Frame 97	24 bytes data	4 bytes C2 error correction	4 bytes C1 error correction	P_{95} Q_{95} R_{95} S_{95} T_{95} U_{95} V_{95} W_{95}

P Channel	P_0	P_1	P_2	.	.	.	.	.	.	.	.	P_{93}	P_{94}	P_{95}
Q Channel	Q_0	Q_1	Q_2	.	.	.	.	.	.	.	.	Q_{93}	Q_{94}	Q_{95}
R Channel	R_0	R_1	R_2	.	.	.	.	.	.	.	.	R_{93}	R_{94}	R_{95}
.	.	.	.									.	.	.
.	.	.	.									.	.	.
.	.	.	.									.	.	.
.	.	.	.									.	.	.
.	.	.	.									.	.	.
.	.	.	.									.	.	.
V Channel	V_0	V_1	V_2	.	.	.	.	.	.	.	.	V_{93}	V_{94}	V_{95}
W Channel	W_0	W_1	W_2	.	.	.	.	.	.	.	.	W_{93}	W_{94}	W_{95}

Figure 4

1 bit	1 bit	4 bit	4 bit	8 bit	8 bit	8 bit	8 bit	8 bit	8 bit	8 bit	8 bit	8bit	16 bit
S0	S1	Control	Address	TNO	X	Min	Sec	Frame	Zero	AMin	ASec	AFrame	CRC

Figure 5

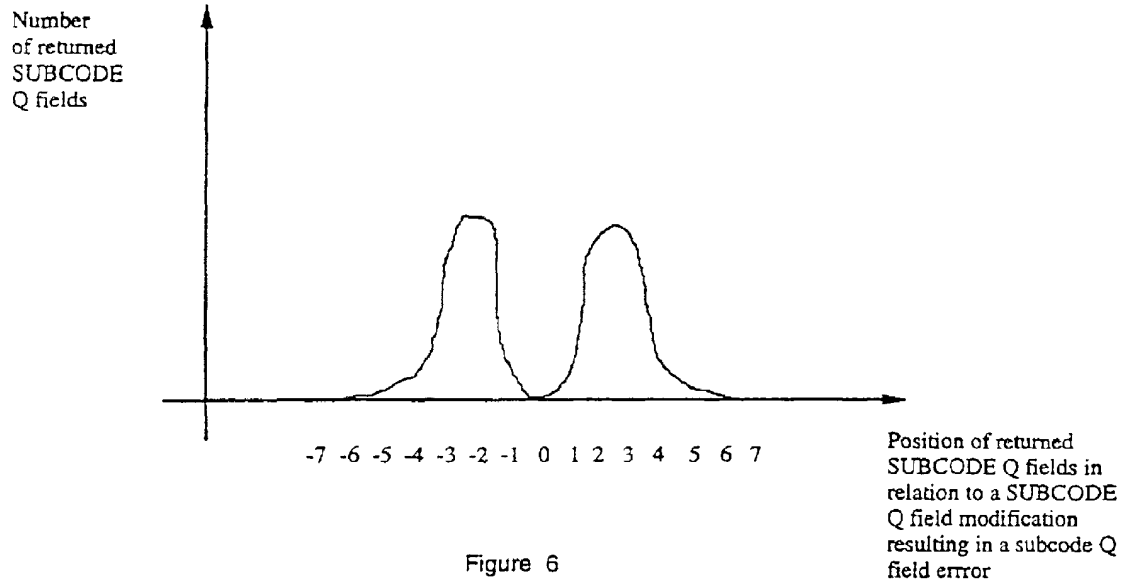

Figure 6

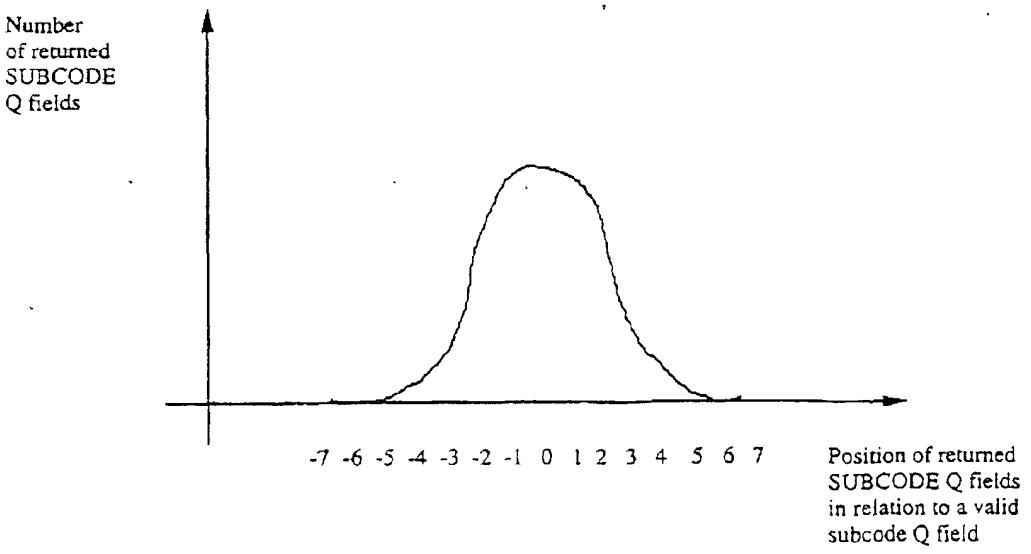

Figure 7

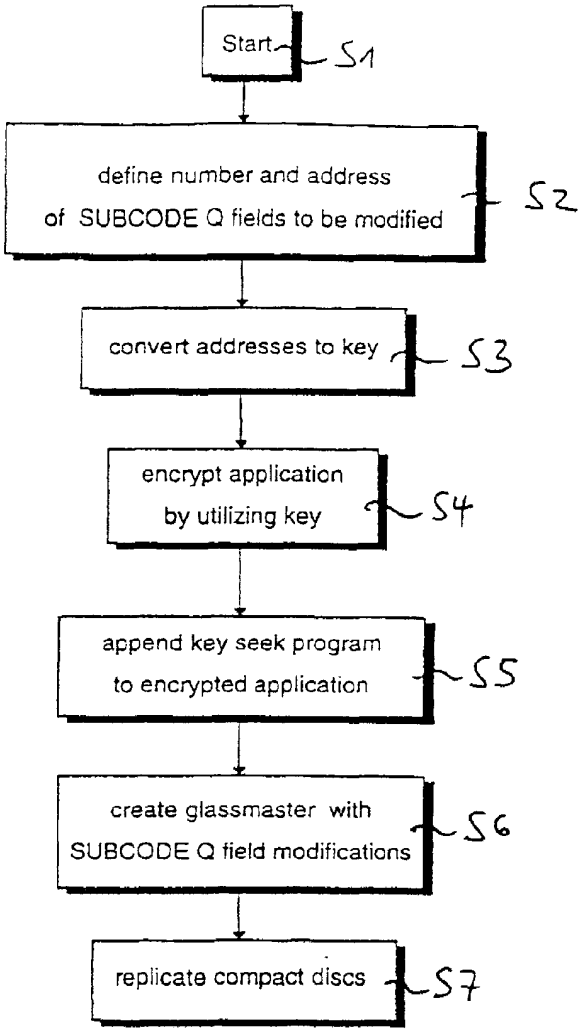
Start
S1
define number and address
of SUBCODE Q fields to be modified
S2
convert addresses to key
S3
encrypt application
by utilizing key
S4
append key seek program
to encrypted application
S5
create glassmaster with
SUBCODE Q field modifications
S6
replicate compact discs
S7

Figure 8

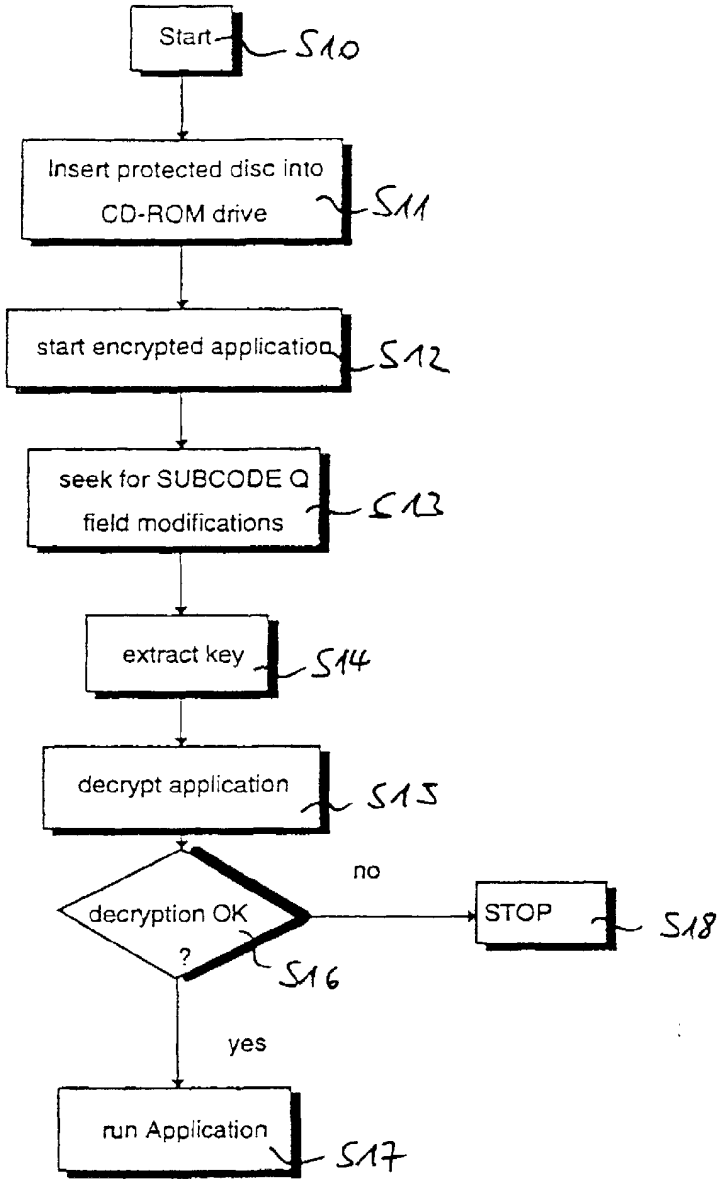
Start
S10
Insert protected disc into CD-ROM drive
S11
start encrypted application
S12
seek for SUBCODE Q field modifications
S13
extract key
S14
decrypt application
S15
decryption OK ?
S16
no
STOP
S18
yes
run Application
S17

Figure 9